PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-140896
(43)Date of publication of application : 02.06.1995

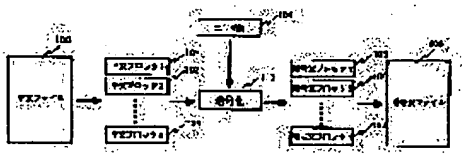
(51)Int.Cl. G09C 1/00
G06F 12/14

(21)Application number : 05-314466
(22)Date of filing : 19.11.1993

(71)Applicant : HITACHI LTD
HITACHI SOFTWARE ENG CO LTD
(72)Inventor : SUZAKI SEIICHI
TAKARAGI KAZUO
NAKAMURA TERUO
NOTOMI MASAHITO

(54) FILE CIPHERING METHOD AND ITS DEVICE

(57)Abstract:
PURPOSE: To adequately cipher a file to be written into a memory device without depending on the kind of an application program by which the file is formed.
CONSTITUTION: The ordinary text file 100 is divided by n to the smallest data size at which data transaction between the data region on a memory to be used by the application program and a disk buffer is possible, by which n-pieces of ordinary text blocks 101 to 103 are formed. Next, n-pieces of these ordinary text blocks 101 to 103 are respectively separately ciphered by a user key 104 and n-pieces of cipher text blocks 105 to 107 are formed. Finally, the formed n-pieces of these cipher text blocks 105 to 107 are connected to obtain a cipher text file 108. Then, the application program ciphers the ordinary text file by each of the smallest data size at which a partial operation, such as superscription, of the file is possible and, therefore, the correct diciphering to the original ordinary text file is possible at any time even if any operation is executed by the application program.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平7－140896

(43)公開日　平成７年(1995)６月２日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０９Ｃ　1/00		9364－5L		
Ｇ０６Ｆ　12/14	３２０　Ｂ			

審査請求　未請求　請求項の数30　ＦＤ　（全 14 頁）

(21)出願番号　特願平5－314466

(22)出願日　平成５年(1993)11月19日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(71)出願人　000233055
日立ソフトウエアエンジニアリング株式会社
神奈川県横浜市中区尾上町６丁目81番地

(72)発明者　洲崎　誠一
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(74)代理人　弁理士　矢島　保夫

最終頁に続く

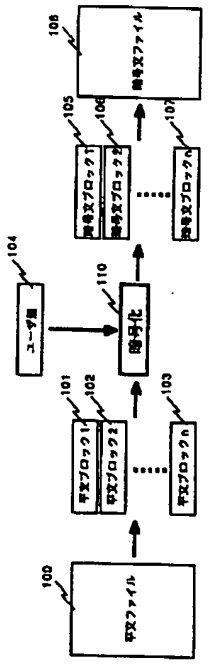
(54)【発明の名称】　ファイル暗号方法及びその装置

(57)【要約】

【目的】ファイルを作成したアプリケーションプログラムの種類に依らず、記憶装置に書き込むファイルを適切に暗号化する。

【構成】まず、アプリケーションプログラムが使用するメモリ上のデータ領域とディスクバッファとの間でデータのやり取りを行なうことができる最も小さなデータサイズに、平文ファイル１００をｎ分割し、ｎ個の平文ブロック１０１、１０２、１０３を生成する。次に、このｎ個の平文ブロック１０１、１０２、１０３を、ユーザ鍵１０４でそれぞれ別々に暗号化し、ｎ個の暗号文ブロック１０５、１０６、１０７を生成する。最後に、生成されたｎ個の暗号文ブロック１０５、１０６、１０７を連結して、暗号文ファイル１０８を得る。

【効果】アプリケーションプログラムが、ファイルに対して、上書き等の部分的操作が可能な最も小さなデータサイズ毎に平文ファイルを暗号化するので、アプリケーションプログラムでどのような操作が行なわれようとも、いつでも元の平文ファイルに正しく復元することができる。



1

【特許請求の範囲】

【請求項１】与えられた平文ファイルを、与えられたユーザ鍵で暗号化し、得られた暗号文ファイルを記憶装置に記憶するとともに、外部からのファイルアクセス指示に応じて該記憶装置にアクセスするファイル暗号方法であって、

与えられた平文ファイルの書き込みの手順が、

書き込みを指示された平文ファイルを、外部からファイルアクセスを指示される際の最も小さなデータサイズまたはそれより小さなデータサイズを単位として分割し、複数個の平文ブロックを生成するステップと、

与えられたユーザ鍵を用いて、該複数個の平文ブロックをそれぞれ別々に暗号化し、複数個の暗号文ブロックを生成するステップと、

該複数個の暗号文ブロックを連結して暗号文ファイルを生成するステップと、

該暗号文ファイルを前記記憶装置に書き込むステップとを備えたことを特徴とするファイル暗号方法。

【請求項２】請求項１に記載のファイル暗号方法において、さらに、

指定された平文ファイルの読み出しの手順が、

該指定された平文ファイルに対応する暗号文ファイルを前記記憶装置から読み出すステップと、

読み出した暗号文ファイルを複数個の暗号文ブロックに分割し、その際、各暗号文ブロックを復号すると元の複数個の平文ブロックが得られるような所定の大きさで分割するステップと、

与えられたユーザ鍵を用いて、該複数個の暗号文ブロックをそれぞれ別々に復号し、複数個の平文ブロックを生成するステップと、

該複数個の平文ブロックを連結して平文ファイルを生成するステップと、

該平文ファイルを出力するステップとを備えたことを特徴とするファイル暗号方法。

【請求項３】請求項１に記載のファイル暗号方法において、さらに、

ユーザ鍵と、平文ファイルを特定する情報と、該平文ファイル内の位置と、該位置に上書きすべき平文データとが与えられたときに、該平文データを上書きする手順が、

上書きを指示された平文データを、前記平文ファイルの分割と同じデータサイズで分割し、複数個の上書き用平文ブロックを生成するステップと、

与えられたユーザ鍵を用いて、該複数個の上書き用平文ブロックをそれぞれ別々に暗号化し、複数個の上書き用暗号文ブロックを生成するステップと、

該複数個の上書き用暗号文ブロックを連結して上書き用暗号文データを生成するステップと、

該上書き用暗号文データを、前記記憶装置の上書きを指示された平文ファイルに対応する暗号文ファイルの上書

2

きを指示された位置に上書きするステップとを備えたことを特徴とするファイル暗号方法。

【請求項４】与えられた平文ファイルを、与えられたユーザ鍵で暗号化し、得られた暗号文ファイルを記憶装置に記憶するとともに、外部からのファイルアクセス指示に応じて該記憶装置にアクセスするファイル暗号方法であって、

与えられた平文ファイルの書き込みの手順が、

書き込みを指示された平文ファイルを、外部からファイルアクセスを指示される際の最も小さなデータサイズまたはそれより小さなデータサイズを単位として分割し、複数個の平文ブロックを生成するステップと、

与えられたユーザ鍵と前記複数個の平文ブロックの各々に固有の情報とから、各平文ブロックにそれぞれ対応する秘密数値であるデータ鍵を生成するステップと、

該複数個のデータ鍵を用いて、前記複数個の平文ブロックをそれぞれ別々に暗号化し、複数個の暗号文ブロックを生成するステップと、

該複数個の暗号文ブロックを連結して暗号文ファイルを生成するステップと、

該暗号文ファイルを前記記憶装置に書き込むステップとを備えたことを特徴とするファイル暗号方法。

【請求項５】請求項４に記載のファイル暗号方法において、さらに、

指定された平文ファイルの読み出しの手順が、

該指定された平文ファイルに対応する暗号文ファイルを前記記憶装置から読み出すステップと、

読み出した暗号文ファイルを複数個の暗号文ブロックに分割し、その際、各暗号文ブロックを復号すると元の複数個の平文ブロックが得られるような所定の大きさで分割するステップと、

与えられたユーザ鍵と前記複数個の平文ブロックの各々に固有の情報とから、各平文ブロックにそれぞれ対応するデータ鍵を生成するステップと、

該複数個のデータ鍵を用いて、前記複数個の暗号文ブロックをそれぞれ別々に復号し、複数個の平文ブロックを生成するステップと、

該複数個の平文ブロックを連結して平文ファイルを生成するステップと、

該平文ファイルを出力するステップとを備えたことを特徴とするファイル暗号方法。

【請求項６】請求項４に記載のファイル暗号方法において、さらに、

ユーザ鍵と、平文ファイルを特定する情報と、該平文ファイル内の位置と、該位置に上書きすべき平文データとが与えられたときに、該平文データを上書きする手順が、

上書きを指示された平文データを、前記平文ファイルの分割と同じデータサイズで分割し、複数個の上書き用平文ブロックを生成するステップと、

3

与えられたユーザ鍵と前記複数個の上書き用平文ブロックの各々に固有の情報とから、各上書き用平文ブロックにそれぞれ対応するデータ鍵を生成するステップと、
該複数個のデータ鍵を用いて、該複数個の上書き用平文ブロックをそれぞれ別々に暗号化し、複数個の上書き用暗号文ブロックを生成するステップと、
該複数個の上書き用暗号文ブロックを連結して上書き用暗号文データを生成するステップと、
該暗号文データを、前記記憶装置の上書きを指示された平文ファイルに対応する暗号文ファイルの上書きを指示された位置に上書きするステップとを備えたことを特徴とするファイル暗号方法。

【請求項７】請求項４から６のいずれか１つに記載のファイル暗号方法において、前記複数個の平文ブロックの各々に固有の情報が、平文ファイルの先頭からその平文ブロックまでのオフセットであることを特徴とするファイル暗号方法。

【請求項８】請求項１から７のいずれか１つに記載のファイル暗号方法において、前記暗号化および復号化は、平文ブロックと暗号文ブロックのデータサイズが同じとなるアルゴリズムを用いて行うことを特徴とするファイル暗号方法。

【請求項９】請求項１から８のいずれか１つに記載のファイル暗号方法において、前記分割、暗号化および復号化は、上位のアプリケーションからアクセスできないワーク領域の上で行うことを特徴とするファイル暗号方法。

【請求項１０】請求項１から９のいずれか１つに記載のファイル暗号方法において、前記ユーザ鍵は、あらかじめユーザに対して配布された個人用記憶媒体に格納されているユーザ鍵を読み出して用いることを特徴とするファイル暗号方法。

【請求項１１】請求項１０に記載のファイル暗号方法において、前記個人用記憶媒体には、前記ユーザ鍵と共に、該個人用記憶媒体を所有するユーザを識別するためのユーザ識別子とパスワードとが記憶されており、該ユーザ識別子とパスワードを使って本人確認処理を行ない、正しいユーザであることが確認されたときにだけ、前記個人用記憶媒体からユーザ鍵を読み出せることを特徴とするファイル暗号方法。

【請求項１２】請求項１１に記載のファイル暗号方法において、前記パスワードの代わりに生物学的特徴によって本人確認処理を行なうことを特徴とするファイル暗号方法。

【請求項１３】請求項１０から１２のいずれか１つに記載のファイル暗号方法において、前記記憶媒体がＩＣカードであることを特徴とするファイル暗号方法。

【請求項１４】請求項１０から１２のいずれか１つに記載のファイル暗号方法において、前記記憶媒体がフロッピーディスクであることを特徴とするファイル暗号方法。

4

【請求項１５】請求項１から１４のいずれか１つに記載のファイル暗号方法において、前記記憶装置が通信網を介して接続されており、前記暗号文ファイルや上書き用暗号文データの書き込みおよび読み出しは、該通信網を介して行われることを特徴とするファイル暗号方法。

【請求項１６】暗号化したファイルを記憶するための記憶装置を備えるとともに、外部からのファイルアクセス指示に応じてファイルアクセスのサービスを実行するファイル暗号装置であって、
書き込みを指示された平文ファイルを、外部からファイルアクセスを指示される際の最も小さなデータサイズまたはそれより小さなデータサイズを単位として分割し、複数個の平文ブロックを生成する手段と、
与えられたユーザ鍵を用いて、該複数個の平文ブロックをそれぞれ別々に暗号化し、複数個の暗号文ブロックを生成する手段と、
該複数個の暗号文ブロックを連結して暗号文ファイルを生成する手段と、
該暗号文ファイルを前記記憶装置に書き込む手段とを備えたことを特徴とするファイル暗号装置。

【請求項１７】請求項１６に記載のファイル暗号装置において、さらに、
読み出しを指定された平文ファイルに対応する暗号文ファイルを前記記憶装置から読み出す手段と、
読み出した暗号文ファイルを複数個の暗号文ブロックに分割し、その際、各暗号文ブロックを復号すると元の複数個の平文ブロックが得られるような所定の大きさで分割する手段と、
与えられたユーザ鍵を用いて、該複数個の暗号文ブロックをそれぞれ別々に復号し、複数個の平文ブロックを生成する手段と、
該複数個の平文ブロックを連結して平文ファイルを生成する手段と、
該平文ファイルを出力する手段とを備えたことを特徴とするファイル暗号装置。

【請求項１８】請求項１６に記載のファイル暗号装置において、さらに、
ユーザ鍵と、平文ファイルを特定する情報と、該平文ファイル内の位置と、該位置に上書きすべき平文データとを入力する手段と、
上書きを指示された平文データを、前記平文ファイルの分割と同じデータサイズで分割し、複数個の上書き用平文ブロックを生成する手段と、
与えられたユーザ鍵を用いて、該複数個の上書き用平文ブロックをそれぞれ別々に暗号化し、複数個の上書き用暗号文ブロックを生成する手段と、
該複数個の上書き用暗号文ブロックを連結して上書き用暗号文データを生成する手段と、
該上書き用暗号文データを、前記記憶装置の上書きを指

5

示された平文ファイルに対応する暗号文ファイルの上書きを指示された位置に上書きする手段とを備えたことを特徴とするファイル暗号装置。

【請求項１９】暗号化したファイルを記憶するための記憶装置を備えるとともに、外部からのファイルアクセス指示に応じてファイルアクセスのサービスを実行するファイル暗号装置であって、

書き込みを指示された平文ファイルを、ファイルアクセスを指示される際の最も小さなデータサイズまたはそれより小さなデータサイズを単位として分割し、複数個の平文ブロックを生成する手段と、

与えられたユーザ鍵と前記複数個の平文ブロックの各々に固有の情報とから、各平文ブロックにそれぞれ対応する秘密数値であるデータ鍵を生成する手段と、

該複数個のデータ鍵を用いて、前記複数個の平文ブロックをそれぞれ別々に暗号化し、複数個の暗号文ブロックを生成する手段と、

該複数個の暗号文ブロックを連結して暗号文ファイルを生成する手段と、

該暗号文ファイルを前記記憶装置に書き込む手段とを備えたことを特徴とするファイル暗号装置。

【請求項２０】請求項１９に記載のファイル暗号装置において、さらに、

読み出しを指定された平文ファイルに対応する暗号文ファイルを前記記憶装置から読み出す手段と、

読み出した暗号文ファイルを複数個の暗号文ブロックに分割し、その際、各暗号文ブロックを復号すると元の複数個の平文ブロックが得られるような所定の大きさで分割する手段と、

与えられたユーザ鍵と前記複数個の平文ブロックの各々に固有の情報とから、各平文ブロックにそれぞれ対応するデータ鍵を生成する手段と、

該複数個のデータ鍵を用いて、前記複数個の暗号文ブロックをそれぞれ別々に復号し、複数個の平文ブロックを生成する手段と、

該複数個の平文ブロックを連結して平文ファイルを生成する手段と、

該平文ファイルを出力する手段とを備えたことを特徴とするファイル暗号装置。

【請求項２１】請求項１９に記載のファイル暗号装置において、さらに、

ユーザ鍵と、平文ファイルを特定する情報と、該平文ファイル内の位置と、該位置に上書きすべき平文データとを入力する手段と、

上書きを指示された平文データを、前記平文ファイルの分割と同じデータサイズで分割し、複数個の上書き用平文ブロックを生成する手段と、

与えられたユーザ鍵と前記複数個の上書き用平文ブロックの各々に固有の情報とから、各上書き用平文ブロックにそれぞれ対応するデータ鍵を生成する手段と、

6

該複数個のデータ鍵を用いて、該複数個の上書き用平文ブロックをそれぞれ別々に暗号化し、複数個の上書き用暗号文ブロックを生成する手段と、

該複数個の上書き用暗号文ブロックを連結して上書き用暗号文データを生成する手段と、

該上書き用暗号文データを、前記記憶装置の上書きを指示された平文ファイルに対応する暗号文ファイルの上書きを指示された位置に上書きする手段とを備えたことを特徴とするファイル暗号装置。

【請求項２２】請求項１９から２１のいずれか１つに記載のファイル暗号装置において、前記複数個の平文ブロックの各々に固有の情報が、平文ファイルの先頭からその平文ブロックまでのオフセットであることを特徴とするファイル暗号装置。

【請求項２３】請求項１６から２２のいずれか１つに記載のファイル暗号装置において、前記ユーザ鍵やデータ鍵を用いて暗号化および復号化を行う各手段は、平文ブロックと暗号文ブロックのデータサイズが同じとなるアルゴリズムを用いて暗号化および復号化を行うことを特徴とするファイル暗号装置。

【請求項２４】請求項１９から２３のいずれか１つに記載のファイル暗号装置において、さらに、上位のアプリケーションからアクセスできないワーク領域を備え、前記分割、暗号化および復号化は該ワーク領域の上で行うことを特徴とするファイル暗号装置。

【請求項２５】請求項１９から２４のいずれか１つに記載のファイル暗号装置において、前記ユーザ鍵は、あらかじめユーザに対して配布された個人用記憶媒体に格納されていることを特徴とするファイル暗号装置。

【請求項２６】請求項２５に記載のファイル暗号装置において、前記個人用記憶媒体には、前記ユーザ鍵と共に、該個人用記憶媒体を所有するユーザを識別するためのユーザ識別子とパスワードとが記憶されており、該ユーザ識別子とパスワードを使って本人確認処理を行ない、正しいユーザであることが確認されたときにだけ、前記個人用記憶媒体からユーザ鍵を読み出せることを特徴とするファイル暗号装置。

【請求項２７】請求項２６に記載のファイル暗号装置において、前記パスワードの代わりに生物学的特徴によって本人確認処理を行なう手段を備えたことを特徴とするファイル暗号装置。

【請求項２８】請求項２５から２７のいずれか１つに記載のファイル暗号装置において、前記記憶媒体がＩＣカードであることを特徴とするファイル暗号装置。

【請求項２９】請求項２５から２７のいずれか１つに記載のファイル暗号装置において、前記記憶媒体がフロッピーディスクであることを特徴とするファイル暗号装置。

【請求項３０】請求項１９から２９のいずれか１つに記載のファイル暗号装置において、前記記憶装置が通信網

7

を介して接続されており、前記暗号文ファイルや上書き用暗号文データの書き込みと読み出しは、該通信網を介して行われることを特徴とするファイル暗号装置。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、パーソナルコンピュータ等の情報処理端末で作成される平文ファイルを適切に暗号化することができるファイル暗号方法及びそのような暗号方法を適用した情報処理システムに関し、更に詳しくは、平文ファイルを作成するために使用するアプリケーションプログラムの種類に依らず、例えば、既に記憶装置に記憶されている暗号文ファイルの一部を上書きした場合でも、元の平文ファイルに正しく復元することができ、また、通信網を介して別の端末の記憶装置に暗号文ファイルを記憶する場合も自端末の記憶装置の場合と同様の安全性を確保することができるファイル暗号方法及び情報処理システムに関する。

【０００２】

【従来の技術】情報機器の発達により、様々な情報が電子的なファイルとして、ハードディスクやフロッピーディスク等の記憶装置に保管されるようになってきている。そのため、機密性の高い情報を含むようなファイルに対しては、暗号化やアクセス制御といったセキュリティ技術を使って情報の保護を行っている。

【０００３】一方、ワークステーションやパソコンを端末としたローカルエリアネットワーク（ＬＡＮ）の普及により、ある端末で作成したファイルを、通信網を介して別の端末の記憶装置に保管する、といったことも行われるようになってきている。

【０００４】ＬＡＮでは、情報は通信回線上を同報的に流れている。すなわち、情報の送信元は、送信すべき情報に相手先のアドレスを付して回線に送信し、回線上の全ての端末でこれを受信する。受信した端末では、そのアドレスを参照して、自分宛の情報であるかどうかをチェックする。したがって、ある端末が同報的に送出した情報は、基本的に、どの端末でも受信可能である。そのため、機密性の高い情報を含むようなファイルを通信網を介して別の端末の記憶装置に保管する場合には、自端末の記憶装置に保管する場合と同様に、暗号化やアクセス制御といったセキュリティ技術を使って、適切に保護する必要がある。

【０００５】従来の暗号方法については、例えば、「現代暗号理論（著：池野　信一、小山謙二；発行：社団法人　電子情報通信学会）」に開示されている。

【０００６】上記開示例では、平文を数バイト程度のブロックに分割し、各ブロックを同一の暗号鍵で暗号化する。何バイト程度のブロックに分割するかは暗号アルゴリズムの種類によって決まるが、通常は６４ビット（８バイト）程度に分割する。

【０００７】この方法は、平文を分割した全ての平文ブロックの暗号化に同一の暗号鍵を用いるので、同一の平文ブロックは同一の暗号文ブロックに変換される。したがって、暗号文ブロックの出現確率から統計的に元の平文ブロックを類推される危険性がある。そのため、暗号文ブロックを平文ブロックと暗号鍵の値に依存させるだけでなく、暗号化しようとする平文ブロックの前にある前平文ブロックや前暗号文ブロックの値にも依存させて暗号文ブロックを作成する手法も広く用いられている。

8

【０００８】ところで、アプリケーションプログラムが、記憶装置にファイルを書き込んだり、記憶装置に保管されているファイルを読み取る場合には、通常、次のような手順で行なわれる。

【０００９】すなわち、アプリケーションプログラムによって指定されたメモリ上のデータ領域にあるファイルは、オペレーティングシステムの制御のもと、一度、ディスクバッファや通信バッファに転送され、その後、自端末、あるいは別の端末の記憶装置に書き込まれる。同様に、既に自端末、あるいは別の端末の記憶装置に保管されているファイルは、一度、ディスクバッファや通信バッファに転送された後、アプリケーションプログラムによって指定されたメモリ上のデータ領域に読み込まれる。

【００１０】ファイル全体ではなく、アプリケーションプログラムを使って、既に自端末、あるいは別の端末の記憶装置に保管されているファイルの一部分のみを修正するような場合にも、ほぼ同様のことが行われる。

【００１１】

【発明が解決しようとする課題】ファイルを作成するためのアプリケーションプログラムは多種多様であり、また、ユーザがそれらのアプリケーションプログラムを使用する環境も多岐にわたっている。そのため、アプリケーションプログラムの種類や、それを使用する環境に依らず、ファイルの暗号化を適切に行うことができるようにしたいといった要求がある。

【００１２】しかし、上記従来技術では、平文ファイルを数バイト程度のブロックに分割して暗号化するので、アプリケーションプログラムが、既に記憶装置に保管されている暗号文ファイルに対し、それより小さなサイズで部分的に上書きした場合に、ブロック内の他のデータとの相関が壊れてしまい、そのブロック全体を正しく復元することができなくなってしまう。

【００１３】また、暗号文ブロックを平文ブロックと暗号鍵の値に依存させるだけでなく、前平文ブロックや前暗号文ブロックの値にも依存させる手法を用いた場合には、上書きにされたブロック以降のブロックは、全て正しく復元することができなくなってしまう。

【００１４】そこで、本発明の一つの目的は、ユーザが使用しているアプリケーションプログラムの種類に依らず、例えば、そのアプリケーションプログラムによって、既に記憶装置に記憶されている暗号文ファイルが部

9

分的に上書きされた場合でも、元の平文ファイルに正しく復元することができるファイル暗号方法及び情報処理システムを提供することにある。

【0015】本発明のもう一つの目的は、暗号文ファイルから元の平文ファイルを類推されてしまう危険性の少ないファイル暗号方法及び情報処理システムを提供することにある。

【0016】本発明の更にもう一つの目的は、通信網を介して別の端末の記憶装置にファイルを保管する場合にも、自端末の記憶装置に保管する場合と同様の安全性を確保することができるファイル暗号方法及び情報処理システムを提供することにある。

【0017】

【課題を解決するための手段】上記の目的を達成するため、本発明に係るファイル暗号方法またはその装置は、与えられた平文ファイルを、与えられたユーザ鍵で暗号化し、得られた暗号文ファイルを記憶装置に記憶するとともに、外部からのファイルアクセス指示に応じて該記憶装置にアクセスする方法または装置であって、与えられた平文ファイルの書き込みは、書き込みを指示された平文ファイルを、外部からファイルアクセスを指示される際の最も小さなデータサイズまたはそれより小さなデータサイズを単位として分割し、複数個の平文ブロックを生成し、与えられたユーザ鍵を用いて、該複数個の平文ブロックをそれぞれ別々に暗号化し、複数個の暗号文ブロックを生成し、該複数個の暗号文ブロックを連結して暗号文ファイルを生成し、該暗号文ファイルを前記記憶装置に書き込むようにする。

【0018】さらに、指定された平文ファイルの読み出しは、該指定された平文ファイルに対応する暗号文ファイルを前記記憶装置から読み出し、読み出した暗号文ファイルを複数個の暗号文ブロックに分割し、その際、各暗号文ブロックを復号すると元の複数個の平文ブロックが得られるような所定の大きさで分割するものとし、与えられたユーザ鍵を用いて、該複数個の暗号文ブロックをそれぞれ別々に復号し、複数個の平文ブロックを生成し、該複数個の平文ブロックを連結して平文ファイルを生成し、該平文ファイルを出力するようにする。

【0019】また、ユーザ鍵と、平文ファイルを特定する情報と、該平文ファイル内の位置と、該位置に上書きすべき平文データとが与えられたときに、該平文データの上書きは、上書きを指示された平文データを、前記平文ファイルの分割と同じデータサイズで分割し、複数個の上書き用平文ブロックを生成し、与えられたユーザ鍵を用いて、該複数個の上書き用平文ブロックをそれぞれ別々に暗号化し、複数個の上書き用暗号文ブロックを生成し、該複数個の上書き用暗号文ブロックを連結して上書き用暗号文データを生成し、該上書き用暗号文データを、前記記憶装置の上書きを指示された平文ファイルに対応する暗号文ファイルの上書きを指示された位置に上

10

書きするようにする。

【0020】さらに、与えられたユーザ鍵を用いて暗号化および復号化を行うのでなく、各ユーザ毎に異なる秘密数値であるユーザ鍵と、平文ファイルの各ブロックに固有の情報（例えば、ファイルの先頭からのオフセット値）等から平文ブロックと同じ個数のデータ鍵を生成し、そのデータ鍵を使って暗号化するようにしてもよい。

【0021】暗号化および復号化は、平文ブロックと暗号文ブロックのデータサイズが同じとなるアルゴリズムを用いるのがよい。平文ファイル上の位置と暗号文ファイル上の位置との対応が簡単に取れる（平文ブロックの平文ファイル先頭からのオフセットと、その平文ブロックに対応する暗号文ブロックの暗号文ファイル先頭からのオフセットとが、同じ）からである。ただし、本発明では、平文ブロックと暗号文ブロックのデータサイズが同じとならないアルゴリズムを用いてもよい。その場合、平文ファイル内の位置と暗号文ファイル内の位置とが相互に変換できるような関数が特定されることが必要になる。

【0022】分割、暗号化および復号化は、上位のアプリケーションからアクセスできないワーク領域の上で行うとよい。上位のアプリケーションの管理下にある領域でこれらの処理を行うと、アプリケーションによっては該領域のデータをさらに表示する処理などを行うことが考えられるからである。

【0023】ユーザ鍵は、あらかじめユーザに対して配布された個人用記憶媒体に格納されているものを用いるとよい。個人用記憶媒体としては、例えば、ＩＣカードやフロッピーディスクを用いる。

【0024】また、個人用記憶媒体にユーザ鍵と共に、該個人用記憶媒体を所有するユーザを識別するためのユーザ識別子とパスワードとを記憶しておき、該ユーザ識別子とパスワードを使って本人確認処理を行ない、正しいユーザであることが確認されたときにだけ、前記個人用記憶媒体からユーザ鍵を読み出せるようにすれば、さらに情報の安全性を確保できる。本人確認処理は、パスワードの代わりに生物学的特徴によって行うようにしてもよい。

【0025】さらに、暗号文ファイルや暗号文データを、通信網を介して接続された記憶装置に、書き込みおよび読み出しするようにしてもよい。

【0026】

【作用】本発明によれば、使用する暗号アルゴリズムの種類に依存した大きさのブロックに平文ファイルを分割するのではなく、例えばアプリケーションプログラムがそのファイルに対して部分的操作のできるデータサイズと同じ、あるいはそれより小さなブロック毎に暗号化しているので、それぞれの暗号文ブロックには相関がなく、たとえアプリケーションプログラムが、既に記憶装

11

置に保管されている暗号文ファイルの一部を上書きした場合においても、元の平文ファイルに正しく復元することができる。

【００２７】また、各平文ブロックをそれぞれ異なるデータ鍵で暗号化する方式によれば、暗号文ブロックを前平文ブロックや前暗号文ブロックの値に依存させなくても、同一の平文ブロックが、必ずしも同一の暗号文ブロックに変換されることはなくなるため、平文ファイルを類推されにくくすることができる。

【００２８】さらに、通信網を介して接続された記憶装置に暗号文ファイルや暗号文データの書き込みおよび読み出しするようにすれば、通信網を流れるデータは暗号化されたデータとなるから、自端末の記憶装置に書き込む場合と同様の安全性を確保することができる。

【００２９】

【実施例】以下、図面を用いて、本発明の実施例を説明する。なお、以下で説明する図面において、同一の番号は同様の部品・要素を表すものとする。また、これにより本発明が限定されるものではない。

【００３０】（実施例１）図１は、本発明の第１の実施例に係るファイル暗号方法による平文ファイルの暗号化手順を示すブロック図である。図２は、本実施例のファイル暗号方法を適用した情報処理システムのシステム構成を示すブロック図である。

【００３１】まず、図２を参照して、本実施例のシステム構成を説明する。

【００３２】図２において、２００はワークステーションやパソコン等の端末である。ユーザは、これらの端末を使って種々の作業を行なう。２１０は、ケーブル２１１によって端末と接続された記憶装置である。ユーザは、アプリケーションプログラムを使って作成したファイルを、この記憶装置２１０に記憶させることができる。また、記憶装置２１０に記憶されているファイルを読み取ることもできる。

【００３３】２２０は、あらかじめ各ユーザに対してそれぞれ１つずつ配布されており、容易に持ち運ぶことができる個人用記憶媒体（例えば、フロッピーディスクやＩＣカード）である。ユーザは、自己の個人用記憶媒体を読み取り装置２３０に差し込んで、作業を行なう。個人用記憶媒体２２０は、読み取り装置２３０とケーブル２３１とを介して端末２００にデータを送る。

【００３４】図３は、端末２００の内部構成図である。同図に示すように、端末２００は、ＣＰＵ（中央処理装置）３０１と、読み取り装置インタフェース３０２と、記憶装置インタフェース３０３と、表示装置３０４と、入力装置３０５と、メモリ３０６とを有している。それらは、バス３００によって相互に接続されている。

【００３５】ＣＰＵ３０１は、種々の演算処理を行なう。読み取り装置インタフェース３０２は、ケーブル２３１を介して読み取り装置２３０から送られてくるデータを受け取るためのインタフェースである。記憶装置インタフェース３０３は、ケーブル２１１を介して記憶装置２１０との間でデータのやり取りを行なうためのインタフェースである。表示装置３０４は、ユーザにメッセージを表示するためのディスプレイ等である。入力装置３０５は、ユーザがデータを入力するためのキーボードやマウス等である。メモリ３０６には、オペレーティングシステム３０７、アプリケーションプログラム３０８、及びセキュリティプログラム３０９等が記憶されている。

12

【００３６】メモリ３０６に記憶されているオペレーティングシステム３０７は、ファイル管理やプロセス管理、あるいはデバイス管理といった機能を提供するために端末全体の制御を行なうプログラム群であり、ディスクバッファやキーボードバッファ等、各種ハードウエアとの間のデータのやり取りを行なうためのデータ領域を有している。アプリケーションプログラム３０８は、ユーザが新規ファイルの作成や既存ファイルの読み取り、書き込み等を行なう際にそれを支援・制御するプログラムである。また、セキュリティプログラム３０９は、ファイルの暗号化及び復号化に係る種々の処理を行なうプログラムである。

【００３７】図４は、個人用記憶媒体２２０の内部構成図である。同図に示すように、個人用記憶媒体２２０には、ユーザ鍵１０４と呼ばれる各個人用記憶媒体に固有の秘密数値が記憶されている。

【００３８】次に、図１を参照して、本実施例において、平文ファイルを暗号化する手順について簡単に説明する。

【００３９】まず、アプリケーションプログラムが使用するメモリ上のデータ領域とディスクバッファとの間でデータのやり取りを行なうことができる最も小さなデータサイズに、平文ファイル１００をｎ分割し、ｎ個の平文ブロック１０１、１０２、１０３を生成する。

【００４０】例えば、その最小データサイズが１バイト、平文ファイルの大きさが１キロバイトである場合、その平文ファイルは１０００個の平文ブロックに分割する。このデータサイズは、その端末で使用可能な全てのアプリケーションプログラムに共通であり、オペレーティングシステムの種類によって、一意に決まる大きさである。

【００４１】次に、このｎ個の平文ブロック１０１、１０２、１０３を、ユーザ鍵１０４でそれぞれ別々に暗号化し、ｎ個の暗号文ブロック１０５、１０６、１０７を生成する。最後に、生成されたｎ個の暗号文ブロック１０５、１０６、１０７を連結して、暗号文ファイル１０８を得る。

【００４２】ただし、本実施例で使用する暗号アルゴリズムは、上記データサイズの平文ブロックを同じ大きさの暗号文ブロックに変換することができる方式（例え

ば、平文と暗号鍵との排他的論理和を暗号文とする方式）である。

【００４３】次に、図５から図７を参照して、本実施例におけるユーザの操作および端末２００の処理について詳しく説明する。

【００４４】図５は、端末２００において、ユーザがアプリケーションプログラム３０８を使用して新規に作成した平文ファイルを暗号化して記憶装置２１０に書き込む場合の処理手順を示す流れ図である。

【００４５】本処理は、ユーザが自己の個人用記憶媒体２２０を読み取り装置２３０に挿入し、アプリケーションプログラム３０８によって作成した平文ファイルを、記憶装置２１０に書き込む操作をすることによって開始される（ステップ５００）。

【００４６】端末２００は、まず、アプリケーションプログラム３０８によって指定されたメモリ上のデータ領域にある平文ファイルのファイルサイズを調べ（ステップ５０１）、それと同じ大きさのデータ領域を新たにメモリ上に確保する（ステップ５０２）。そして、そのデータ領域に平文ファイルを複写する（ステップ５０３）。

【００４７】次に、複写した平文ファイルをｎ個の平文ブロックに分割する（ステップ５０４）。平文ブロックのデータサイズは、図１で説明したように、アプリケーションプログラムが使用するメモリ上のデータ領域とディスクバッファとの間でデータのやり取りを行なうことができる最も小さなデータサイズである。このデータサイズは、オペレーティングシステムの種類によって一意に決まっている。

【００４８】そして、個人用記憶媒体２２０よりユーザ鍵を読み取り（ステップ５０５）、そのユーザ鍵で、ｎ個の平文ブロックをそれぞれ別々に暗号化する（ステップ５０６）。ユーザ鍵は、あらかじめ個人用記憶媒体が挿入された時点で、メモリ上の決められた領域に読み取っておいてもよい。

【００４９】更に、生成されたｎ個の暗号文ブロックを連結し（ステップ５０７）、一つの暗号文ファイルとした後、本来、平文ファイルを転送するはずであったディスクバッファに、暗号文ファイルを転送して、記憶装置２１０に書き込む（ステップ５０８）。このとき、転送する暗号文ファイルのファイルサイズがディスクバッファの大きさより大きな場合には、ステップ５０８を繰り返し実行する。

【００５０】最後に、ユーザが読み取り装置２３０から個人用記憶媒体２２０を取り出すことによって全ての処理が終了する（ステップ５０９）。

【００５１】図６は、端末２００において、ユーザがアプリケーションプログラム３０８を使用して既に記憶装置２１０に記憶されている暗号文ファイルの一部を上書きする場合の処理手順を示す流れ図である。

【００５２】本処理は、ユーザが自己の個人用記憶媒体２２０を読み取り装置２３０に挿入し、アプリケーションプログラム３０８によって作成した、上書きしようとする平文データを、記憶装置２１０に書き込む操作をすることによって開始される（ステップ６００）。

【００５３】端末２００は、まず、アプリケーションプログラム３０８によって指定されたメモリ上のデータ領域にある上書きすべき平文データのデータサイズを調べ（ステップ６０１）、それと同じ大きさのデータ領域を新たにメモリ上に確保する（ステップ６０２）。そして、そのデータ領域に平文データを複写する（ステップ６０３）。

【００５４】次に、複写した平文データをｍ個の平文ブロックに分割する（ステップ６０４）。平文ブロックのデータサイズは、図１あるいは図５でも説明したように、アプリケーションプログラムが使用するメモリ上のデータ領域とディスクバッファとの間でデータのやり取りを行なうことができる最も小さなデータサイズである。

【００５５】そして、個人用記憶媒体２２０よりユーザ鍵を読み取り（ステップ６０５）、そのユーザ鍵で、ｍ個の平文ブロックをそれぞれ別々に暗号化する（ステップ６０６）。本処理でも、あらかじめ個人用記憶媒体が挿入された時点で、ユーザ鍵をメモリ上の決められた領域に読み取っておいてもよい。

【００５６】更に、生成されたｍ個の暗号文ブロックを連結し（ステップ６０７）、一つの暗号文データとした後、本来、平文データを転送するはずであったディスクバッファに、暗号文データを転送して、記憶装置２１０に上書きする（ステップ６０８）。このとき、転送する暗号文データのデータサイズがディスクバッファの大きさより大きな場合には、ステップ６０８を繰り返し実行する。

【００５７】最後に、ユーザが読み取り装置２３０から個人用記憶媒体２２０を取り出すことによって全ての処理が終了する（ステップ６０９）。

【００５８】図７は、端末２００において、ユーザがアプリケーションプログラム３０８を使用して既に記憶装置２１０に書き込まれている暗号文ファイルを読み取る場合の処理手順を示す流れ図である。

【００５９】本処理は、ユーザが自己の個人用記憶媒体２２０を読み取り装置２３０に挿入し、アプリケーションプログラム３０８によって、記憶装置２１０に書き込まれている暗号文ファイルを読み取る操作をすることによって開始される（ステップ７００）。

【００６０】端末２００は、まず、記憶装置２１０に記憶されている暗号文ファイルのファイルサイズを調べ（ステップ７０１）、それと同じ大きさのデータ領域を新たにメモリ上に確保する（ステップ７０２）。そして、本来、アプリケーションプログラム３０８によって

15

指定されたメモリ上のデータ領域に読み込まれるべき暗号文ファイルを、記憶装置２１０から、ディスクバッファを介して、新たに確保したデータ領域に読み取る（ステップ７０３）。このとき、転送する暗号文ファイルのファイルサイズがディスクバッファの大きさより大きな場合には、ステップ７０３の処理を繰り返し実行する。

【００６１】次に、読み込まれた暗号文ファイルをｎ個の暗号文ブロックに分割する（ステップ７０４）。上述したように、本実施例で使用する暗号アルゴリズムは平文ブロックと暗号文ブロックとが同じ大きさになるような方式であるから、この暗号文ブロックのデータサイズは、図１および図５で説明したｎ個に分割した平文ブロックのデータサイズと同じということになる。

【００６２】そして、個人用記憶媒体２２０よりユーザ鍵を読み取り（ステップ７０５）、そのユーザ鍵で暗号文ブロックをそれぞれ別々に復号する（ステップ７０６）。本処理でも、あらかじめ個人用記憶媒体が挿入された時点で、ユーザ鍵をメモリ上の決められた領域に読み取っておいてもよい。

【００６３】更に、ｎ個の平文ブロックを連結し（ステップ７０７）、一つの平文ファイルとした後、アプリケーションプログラム３０８によって指定されたメモリ上のデータ領域にこの平文ファイルを転送する（ステップ７０８）

【００６４】最後に、ユーザが読み取り装置２３０から個人用記憶媒体２２０を取り出すことによって全ての処理が終了する（ステップ７０９）。

【００６５】上述の実施例では、平文ファイルの暗号化を行なうときに、アプリケーションプログラムの種類によって変わるような情報を使っていないので、ユーザが、その端末で使用可能な、どのようなアプリケーションプログラムを使用して平文ファイルを作成した場合においても、同じように暗号化することができる。

【００６６】また、全ての平文ブロックをそれぞれ別々に暗号化しているので、各暗号文ブロックの間に相関はない。したがって、既に記憶装置に記憶されている暗号文ファイル、すなわち連結された暗号文ブロックの一部に対し、新たに作成した暗号文ブロックを上書きした場合においても、他の暗号文ブロックが破壊されることはなく、元の平文ファイルに正しく復元することができる。

【００６７】更に、各個人用記憶媒体毎に異なるユーザ鍵を使って暗号化を行なっているので、平文ファイルを暗号化した本人以外のユーザが、記憶装置に記憶されている暗号文ファイルを復号して、正しい平文ファイルを手に入れることはできない。

【００６８】なお、図８に示すように、個人用記憶媒体２２０にユーザＩＤ８００（各ユーザごとに異なる個人識別子）やパスワード８０１をユーザ鍵１０４と共に記憶しておき、ユーザが個人用記憶媒体を使用する際に、

16

パスワードによる本人確認処理を行なうようにすることによって、更に安全性を高めることができる。その際、パスワードの代わりに、指紋等の各ユーザの生物学的特徴を使用して本人確認処理を行なっても同様の効果が得られる。

【００６９】また、上記実施例では平文ブロックと暗号文ブロックとが同じ大きさとなるような暗号アルゴリズムを用いたが、これに限らず、平文ブロックと暗号文ブロックとが同じ大きさとならない暗号アルゴリズムを用いてもよい。この場合、平文ファイル内のデータの位置と暗号文ファイル内の位置とが、対応付けられるようになっていることが必要である。

【００７０】（実施例２）次に、本発明の第２の実施例を説明する。第２の実施例は、基本的には上述の第１の実施例と同様である。そのシステム構成、及び端末の内部構成は、上述の第１の実施例の図２、３と同様である。また、個人用記憶媒体の内部構成も図４と同様である。

【００７１】図９は、本実施例における平文ファイルの暗号化手順を示すブロック図である。図９において、図１と同じ処理あるいは情報には同じ番号を付して説明を省略する。図９が図１と異なる点は、ブロック９００から９０５、及び９１０である。

【００７２】本実施例では、各平文ブロック１０１、１０２、１０３を同一のユーザ鍵１０４で暗号化するのではなく、ユーザ鍵１０４と各平文ブロックに固有の値とから、平文ブロックと同じ個数のデータ鍵９０３、９０４、９０５を生成し、そのデータ鍵９０３、９０４、９０５で各平文ブロック１０１、１０２、１０３をそれぞれ別々に暗号化する。

【００７３】平文ブロック１０１はデータ鍵９０３で暗号化し、平文ブロック１０２はデータ鍵９０４で暗号化し、…、平文ブロック１０３はデータ鍵９０５で暗号化し、というようにする。各平文ブロックに固有の値としては、例えば、同図に示すように、各平文ブロックの平文ファイルの先頭からのオフセット値９００、９０１、９０２が用いられる。

【００７４】図１０は、端末２００において、ユーザがアプリケーションプログラム３０８を使用して新規に作成した平文ファイルを、暗号化して記憶装置２１０に書き込む場合の処理手順を示す流れ図である。これは基本的には図５と同様の手順である。

【００７５】ただし、個人用記憶媒体２２０、あるいはメモリ上の決められたデータ領域からユーザ鍵を読み取った（ステップ５０５）後、そのユーザ鍵と各平文ブロックの平文ファイルの先頭からのオフセット値より、ｎ個のデータ鍵を生成し（ステップ１０００）、そのｎ個のデータ鍵でｎ個の平文ブロックをそれぞれ別々に暗号化する（ステップ１００１）、という点が異なる。

【００７６】図１１は、端末２００において、ユーザが

17

アプリケーションプログラム３０８を使用して、既に記憶装置２１０に記憶されている暗号文ファイルの一部を上書きする場合の処理手順を示す流れ図である。これは基本的には図６と同様の手順である。

【００７７】ただし、個人用記憶媒体２２０、あるいはメモリ上の決められたデータ領域からユーザ鍵を読み取った（ステップ６０５）後、そのユーザ鍵と各平文ブロックの平文ファイルの先頭からのオフセット値より、ｍ個のデータ鍵を生成し（ステップ１１００）、そのｍ個のデータ鍵でｍ個の平文ブロックをそれぞれ別々に暗号化する（ステップ１１０１）、という点が異なる。

【００７８】本実施例では、データ鍵を生成するために上書きすべきデータの先頭からのオフセット値ではなく、元の平文ファイルの先頭からのオフセット値を使用している。したがって、ここで使用するｍ個のデータ鍵の値は、上書きする位置に記憶されている元の暗号文ブロックを生成するときに使用したデータ鍵の値と同じであることは明らかである。

【００７９】図１２は、端末２００において、ユーザがアプリケーションプログラム３０８を使用して、既に記憶装置２１０に記憶されている暗号文ファイルを読み取る場合の処理手順を示す流れ図である。これは基本的には図７と同様の手順である。

【００８０】ただし、個人用記憶媒体２２０、あるいはメモリ上の決められたデータ領域からユーザ鍵を読み取った（ステップ７０５）後、そのユーザ鍵と各暗号文ブロックの暗号文ファイルの先頭からのオフセット値（平文ファイルの先頭からのオフセット値と同じ値）より、ｎ個のデータ鍵を生成し（ステップ１２００）、そのｎ個のデータ鍵でｎ個の暗号文ブロックをそれぞれ別々に復号する（ステップ１２０１）、という点が異なる。

【００８１】第１の実施例では、各平文ブロックを同一のユーザ鍵で暗号化していた。これに対し、本実施例では、一つのユーザ鍵から平文ブロックと同数のデータ鍵を生成し、そのデータ鍵で各平文ブロックをそれぞれ別々に暗号化している。したがって、第１の実施例と同様の効果が得られるほかに、個人用記憶媒体に記憶する情報を変更しなくても、同一の平文ブロックが必ず同一の暗号文ブロックに変換されるということがなくなるので、平文ファイルを類推されにくくすることができる。

【００８２】（実施例３）次に、本発明の第３の実施例を説明する。第３の実施例は、基本的には上述の第２の実施例と同様である。ただし、各端末が通信網を介して相互に接続されており、アプリケーションプログラムを使って作成したファイルを、別の端末の記憶装置に書き込むことが可能である点が異なる。

【００８３】図１３は、本実施例のシステム構成を示すブロック図である。

【００８４】図１３において、一つ一つの端末と、それと共に使用される記憶装置、読み取り装置、及び個人用

18

記憶媒体は、基本的に図２のそれと同じである。ただし、複数の端末２００が通信網１３００によって相互に接続されている点が異なる。

【００８５】図１４は、本実施例の端末の内部構成を示すブロック図である。これは基本的に図３と同じである。ただし、端末２００が、通信網１３００を介して別の端末との間でデータのやり取りを行なうための通信網インタフェース１４００を有している点と、メモリ３０６にそれを制御するための通信制御プログラム１４０１が記憶されている点とが異なる。

【００８６】図１５は、端末２００において、ユーザがアプリケーションプログラム３０８を使用して新規に作成した平文ファイルを、暗号化して、別の端末の記憶装置２１０に書き込む場合の処理手順を示す流れ図である。これは基本的には図１０と同様の手順である。ただし、ディスクバッファではなく、通信バッファを介して、別の端末の記憶装置２１０に暗号文ファイルを書き込む点が異なっている（ステップ１５００）。

【００８７】図１６は、端末２００において、ユーザがアプリケーションプログラム３０８を使用して、既に別の端末の記憶装置２１０に記憶されている暗号文ファイルの一部を上書きする場合の処理手順を示す流れ図である。これは基本的には図１１と同様の手順である。ただし、ディスクバッファではなく、通信バッファを介して、別の端末の記憶装置２１０に暗号文データを上書きする点が異なっている（ステップ１６００）。

【００８８】図１７は、端末２００において、ユーザがアプリケーションプログラム３０８を使用して、既に別の端末の記憶装置２１０に記憶されている暗号文ファイルを読み取る場合の処理手順を示す流れ図である。これは基本的には図１２と同様の手順である。ただし、ディスクバッファではなく、通信バッファを介して、別の端末の記憶装置２１０から暗号文ファイルを読み取る点が異なっている（ステップ１７００）。

【００８９】本実施例では、通信バッファに転送される以前にデータが暗号化されているので、通信網には暗号化されたデータだけが流れることになる。したがって、第２の実施例と同様の効果が得られるほかに、通信網を介して別の端末の記憶装置にファイルを書き込むような場合にも、自端末の場合と同様の安全性を確保することができる。

【００９０】

【発明の効果】以上説明したように、本発明によれば、アプリケーションプログラムによって指定されたメモリ上のデータ領域からディスクバッファにデータを転送することができる最も小さなデータサイズと同じ大きさ（オペレーティングシステムの種類に依って一意に決まる大きさ）でファイルを暗号化しているので、使用するアプリケーションの種類に依らず、例えば、そのアプリケーションプログラムが、既に記憶装置に記憶されてい

19

る暗号文ファイルの一部を上書きした場合でも、元の平文ファイルに正しく復元することができる。

【００９１】また、各平文ブロックを、それらの平文ブロックと同じ個数のデータ鍵で暗号化した場合には、同一の平文ブロックが、必ずしも同一の暗号文ブロックには変換されないので、平文ファイルを類推されにくくなり、安全性を高めることができる。

【００９２】更に、アプリケーションプログラムによって指定されたメモリ上のデータ領域にある平文ファイルが、通信バッファに転送されたときには既に暗号化されているので、通信網には暗号文ファイルが流れることになり、通信網を介して別の端末の記憶装置に暗号文ファイルを書き込む場合にも、自端末の記憶装置に書き込む場合と同様の安全性を確保することができる。

【図面の簡単な説明】

【図１】本発明の第１の実施例を示すブロック図である。

【図２】第１の実施例のシステム構成図である。

【図３】第１の実施例における端末の内部構成図である。

【図４】第１の実施例における個人用記憶媒体の内部構成図である。

【図５】第１の実施例において、新規に作成した平文ファイルを暗号化する場合の処理手順を示す流れ図である。

【図６】第１の実施例において、記憶装置に記憶された暗号文ファイルに上書きする場合の処理手順を示す流れ図である。

【図７】第１の実施例において、暗号文ファイルを復号する場合の処理手順を示す流れ図である。

20

【図８】第１の実施例の変形例における個人用記憶媒体の内部構成図である。

【図９】本発明の第２の実施例を示すブロック図である。

【図１０】第２の実施例において、新規に作成した平文ファイルを暗号化する場合の処理手順を示す流れ図である。

【図１１】第２の実施例において、記憶装置に記憶された暗号文ファイルに上書きする場合の処理手順を示す流れ図である。

【図１２】第２の実施例において、暗号文ファイルを復号する場合の処理手順を示す流れ図である。

【図１３】本発明の第３の実施例のシステム構成図である。

【図１４】第３の実施例における端末の内部構成図である。

【図１５】第３の実施例において、新規に作成した平文ファイルを暗号化する場合の処理手順を示す流れ図である。

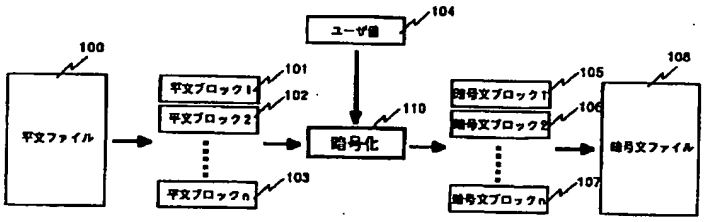
【図１６】第３の実施例において、記憶装置に記憶された暗号文ファイルに上書きする場合の処理手順を示す流れ図である。

【図１７】第３の実施例において、暗号文ファイルを復号する場合の処理手順を示す流れ図である。

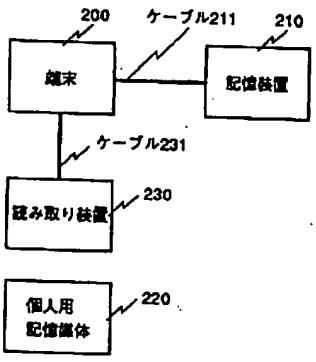
【符号の説明】

２００…端末、
２１０…記憶装置、
２２０…個人用記憶媒体、
２３０…読み取り装置、
１３００…通信網。

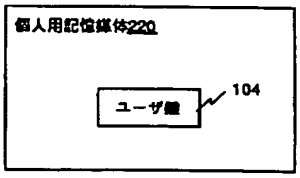
【図１】



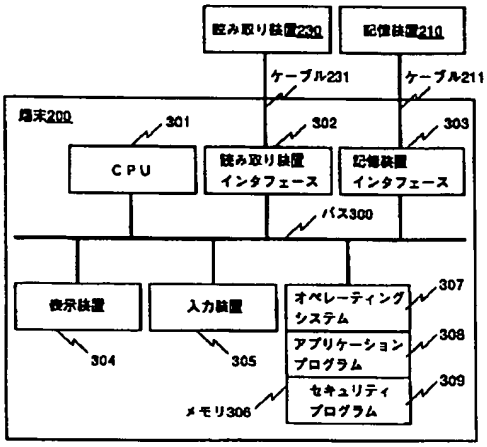
【図２】



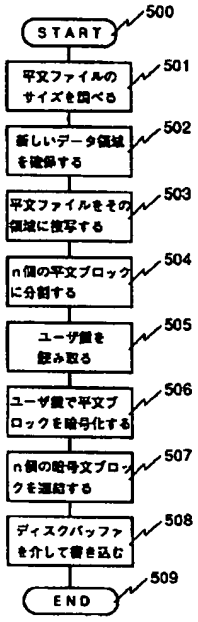
【図４】



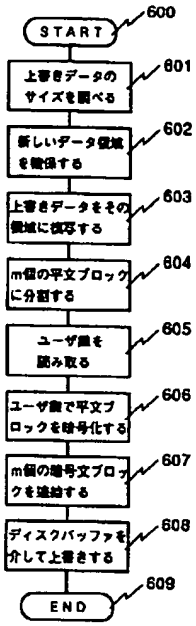
【図３】



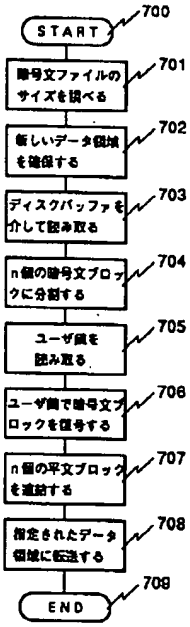
【図５】



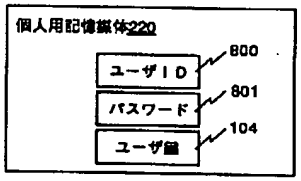
【図６】



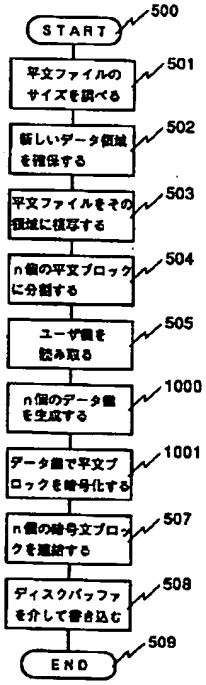
【図７】



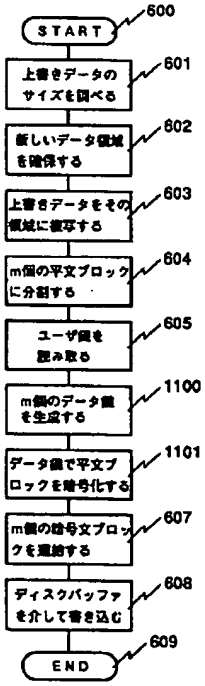
【図８】



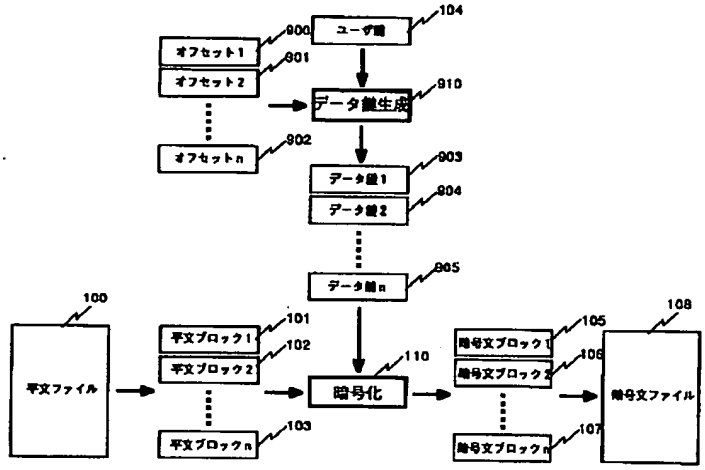
【図１０】



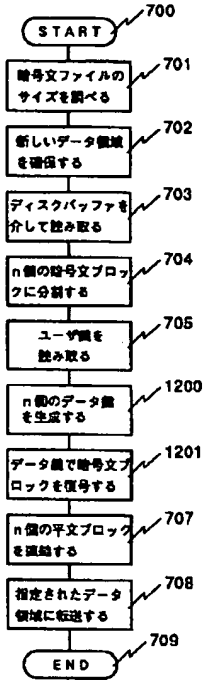
【図１１】



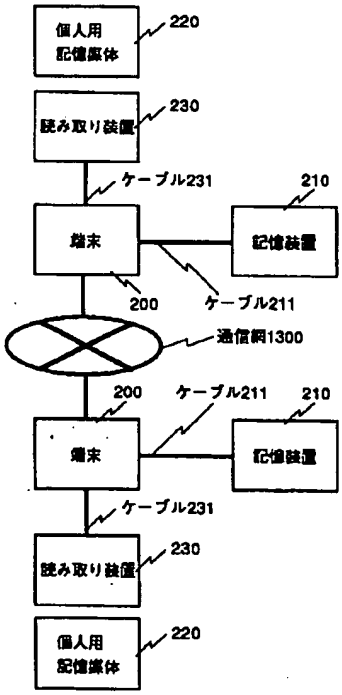
【図９】



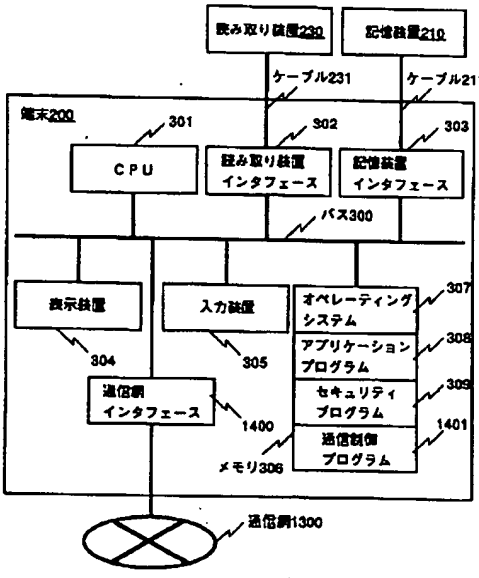
【図１２】



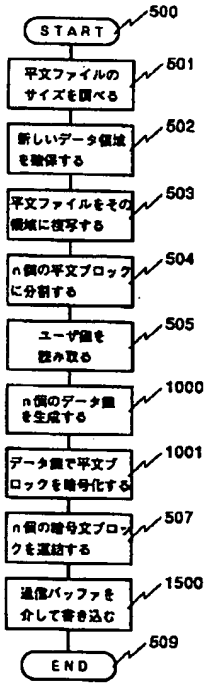
【図１３】



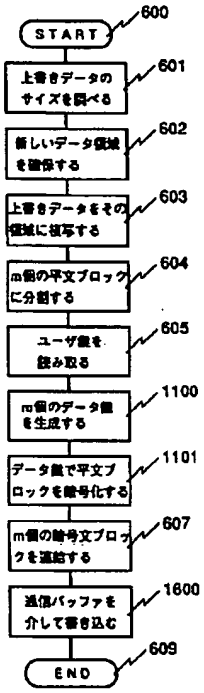
【図１４】



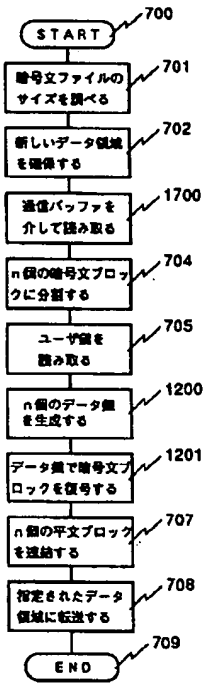
【図１５】



【図１６】



【図１７】



フロントページの続き

(72) 発明者　宝木　和夫
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(72) 発明者　中村　輝雄
神奈川県横浜市中区尾上町６丁目81番地　日立ソフトウェアエンジニアリング株式会社内

(72) 発明者　納富　雅人
神奈川県横浜市中区尾上町６丁目81番地　日立ソフトウェアエンジニアリング株式会社内